PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-175476
(43)Date of publication of application : 02.07.1999

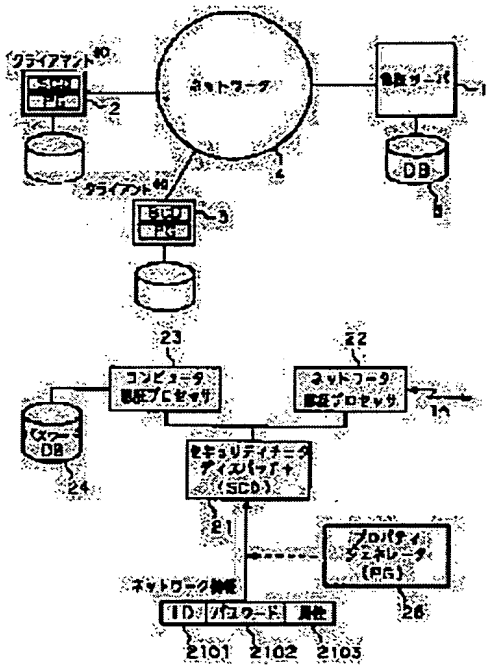
(51)Int.Cl. G06F 15/00
G06F 13/00
H04L 9/32

(21)Application number : 09-346454
(22)Date of filing : 16.12.1997

(71)Applicant : TOSHIBA CORP
(72)Inventor : HOSHINA SATOSHI

(54) SECURITY CHECK METHOD AND AUTHENTICATION SYSTEM AND RECORD MEDIUM FOR RECORDING PROGRAM IN THE SAME METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To realize synthetic security management by providing pleural authentication systems, and selecting and executing the certification system according to attribute information other than a user name and a password inputted by a user.
SOLUTION: When a computer 2(3) uses a computer resource or a network resource, a security check dispatcher 21 promotes the input of network information including attribute information in addition to a user identifier and a password, selects any of plural proliminairly prepared certification systems according to the inputted attribute information or constitution information following a PD 5, and activates a computer authenticating processor 23 or a network authenticating processor 22. Thus, security check following the selected certification system can be attained.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－175476

(43)公開日　平成11年(1999)７月２日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ
13/00	３５１	13/00	３５１Ｚ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ

審査請求　未請求　請求項の数８　ＯＬ　（全 ５ 頁）

(21)出願番号　特願平9－346454

(22)出願日　平成９年(1997)12月16日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　保科　聡
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

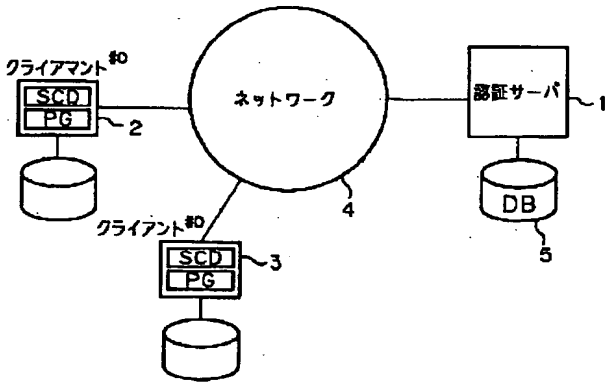
(74)代理人　弁理士　大胡　典夫　（外１名）

(54)【発明の名称】　セキュリティチェック方法ならびに認証システム、及び同方法のプログラムが記録される記録媒体

(57)【要約】

【課題】　本発明は、複数の認証方式を備え、ユーザが入力するユーザ名とパスワード以外の属性情報に従いその認証方式を選択実行することにより、統一したセキュリティ管理を実現することを主な課題とする。

【解決手段】　セキュリティチェックディスパッチャ２１は、そのコンピュータ２（３）が、コンピュータ資源あるいはネットワーク資源を使用する場合、ユーザ識別子とパスワードの他にその属性情報を含むネットワーク情報の入力を促し、入力される属性情報あるいはＰＤ２５に従う構成情報に従い、あらかじめ準備される複数の認証方式のうちいずれかを選択し、コンピュータ認証プロセッサ２３あるいはネットワーク認証プロセッサ２２を起動し、選択された認証方式に従うセキュリティチェックを行う。



1

【特許請求の範囲】

【請求項1】　ネットワークと接続することでネットワーク内資源を使用できるコンピュータであって、そのコンピュータがコンピュータ資源あるいはネットワーク資源を使用する場合、ユーザ識別子とパスワードの他にその属性情報を含むネットワーク情報の入力を促し、入力される属性情報に従い、あらかじめ準備される複数の認証方式のうちいずれかを選択し、選択された認証方式に従うセキュリティチェックを行うことを特徴とするセキュリティチェック方法。

【請求項2】　ネットワークと接続することでネットワーク内資源を使用できるコンピュータであって、そのコンピュータがコンピュータ資源あるいはネットワーク資源を使用する場合、システムが持つ構成情報を基に、あらかじめ準備される複数の認証方式のうちのいずれか選択し、入力されるユーザ識別子とパスワードにより、選択された認証方式に従うセキュリティチェックを行うことを特徴とするセキュリティチェック方法。

【請求項3】　ある認証方式にてアクセスが可能となった資源は、他の認証方式にてアクセス可能になった資源を含むことを特徴とする請求項1もしくは2記載のセキュリティチェック方法。

【請求項4】　ユーザによる属性情報の設定よりも、システムが持つ構成情報による属性情報の設定を優先することを特徴とする請求項2記載のセキュリティチェック方法。

【請求項5】　ユーザ識別子とパスワードの他にその属性情報を含むネットワーク情報の入力を促し、入力される属性情報に従い、あらかじめ準備される複数の認証方式のうちいずれかを選択し、自身で認証、もしくはネットワーク回線を介して接続される認証サーバに対して認証を委ねる１台以上のコンピュータと、属性情報によっては認証を行い要求のあったコンピュータに対してその認証の結果を応答する認証サーバとを具備することを特徴とする認証システム。

【請求項6】　システムによって生成される構成情報を基に、あらかじめ準備される複数の認証方式のうちのいずれか選択し、入力されるユーザ識別子とパスワードにより自身で認証するか、もしくはネットワーク回線を介して接続される認証サーバに対して認証を委ねる１台以上のコンピュータと、構成情報によっては認証を行い要求のあったコンピュータに対してその認証の結果を応答する認証サーバとを具備することを特徴とする認証システム。

【請求項7】　ネットワークと接続することでネットワーク内資源を使用できるコンピュータに用いられる記録媒体であって、そのコンピュータがコンピュータ資源あるいはネットワーク資源を使用する場合において用いられ、ユーザ識別子とパスワードの他にその属性情報を含むネットワーク情報の入力を促すステップと、入力される属性情報に従い、あらかじめ準備される複数の認証方式のうちいずれかを選択するステップと、選択された認証方式に従うセキュリティチェックを行うステップのプログラム情報が記録されるコンピュータ読取り可能な記録媒体。

2

【請求項8】　ネットワークと接続することでネットワーク内資源を使用できるコンピュータに用いられる記録媒体であって、そのコンピュータがコンピュータ資源あるいはネットワーク資源を使用する場合において用いられ、システムにより生成される構成情報を参照するステップと、構成情報を基に、あらかじめ準備される複数の認証方式のうちのいずれか選択するステップと、入力されるユーザ識別子とパスワードにより、選択された認証方式に従うセキュリティチェックを行うステップのプログラム情報が記録されるコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、セキュリティチェック方法ならびに認証システム、及び同方法がプログラムされ記録される記録媒体に関する。

【０００２】

【従来の技術】クライアントサーバシステムにおいては、ユーザ側のインタフェース、及びアプリケーションロジックを持つクライアントシステムから、データベースアクセス等特定の機能を持つサーバをアクセスし、そのサーバで、もしくはネットワークを介した他の異なるコンピュータ上で処理し、クライアントの要求に答えることにより、ネットワーク接続されたコンピュータ間で連携してシステムを実現する。

【０００３】ところで、上述したクライアントサーバシステムは、ネットワーク資源、ネットワークを構築する各コンピュータ資源のそれぞれのセキュリティを管理する必要がある。従来、これらの資源は、セキュリティ的には別々に管理されており、複数の資源群をアクセスするには、複数のセキュリティチェックをユーザに強いてきた。

【０００４】

【発明が解決しようとする課題】これらを統合する方法として、単純に一つのセキュリティ方式にてその複数の資源をアクセスできるようにする方法も考えられるが、この場合、通常は、ネットワーク側のセキュリティ情報を使わざるをえない。

【０００５】例えば、特開昭8－３１４８６３号では、ネットワークの認証はネットワーク上で行われるが、以降の資源のアクセス権のチェックは、本体側のコンピュータで行なうようにしたものである。このようにして一括したセキュリティを確保する方法もあるが、この場合、そのコンピュータがネットワークから切り離された場合もネットワークのセキュリティチェックが必要にな

る。即ち、必要もないのにネットワーク上に認証情報が流れる。また、そうではなく、本体だけのセキュリティチェックを行なう場合、上述した複数のセキュリティチェックを受けることと同じである。

【０００６】本発明は上記事情に鑑みてなされたものであり、複数の認証方式を備え、ユーザが入力するユーザ名とパスワード以外の属性情報に従いその認証方式を選択実行することにより、統一したセキュリティ管理を実現することのできる、セキュリティチェック方法ならびに認証システム、及び同方法がプログラムされ記録される記録媒体を提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明のセキュリティチェック方法は、ネットワークと接続することでネットワーク内資源を使用できるコンピュータであって、そのコンピュータがコンピュータ資源あるいはネットワーク資源を使用する場合、ユーザ識別子とパスワードの他にその属性情報を含むネットワーク情報の入力を促し、入力される属性情報に従い、あらかじめ準備される複数の認証方式のうちいずれかを選択し、選択された認証方式に従うセキュリティチェックを行うことを特徴とする。また、ネットワークと接続することでネットワーク内資源を使用できるコンピュータであって、そのコンピュータがコンピュータ資源あるいはネットワーク資源を使用する場合、システムが持つ構成情報を基に、あらかじめ準備される複数の認証方式のうちのいずれか選択し、入力されるユーザ識別子とパスワードにより、選択された認証方式に従うセキュリティチェックを行うことも特徴とする。

【０００８】本発明の認証システムは、ユーザ識別子とパスワードの他にその属性情報を含むネットワーク情報の入力を促し、入力される属性情報に従い、あらかじめ準備される複数の認証方式のうちいずれかを選択し、自身で認証、もしくはネットワーク回線を介して接続される認証サーバに対して認証を委ねる１台以上のコンピュータと、属性情報によっては認証を行い要求のあったコンピュータに対してその認証の結果を応答する認証サーバとを具備することを特徴とする。また、システムによって生成される構成情報を基に、あらかじめ準備される複数の認証方式のうちのいずれか選択し、入力されるユーザ識別子とパスワードにより自身で認証するか、もしくはネットワーク回線を介して接続される認証サーバに対して認証を委ねる１台以上のコンピュータと、構成情報によっては認証を行い要求のあったコンピュータに対してその認証の結果を応答する認証サーバとを具備することも特徴とする。

【０００９】本発明の記録媒体は、ネットワークと接続することでネットワーク内資源を使用できるコンピュータであって、そのコンピュータがコンピュータ資源あるいはネットワーク資源を使用する場合において用いられ、ユーザ識別子とパスワードの他にその属性情報を含むネットワーク情報の入力を促すステップと、入力される属性情報に従い、あらかじめ準備される複数の認証方式のうちいずれかを選択するステップと、選択された認証方式に従うセキュリティチェックを行うステップとがプログラムされ記録される。また、ネットワークと接続することでネットワーク内資源を使用できるコンピュータであって、そのコンピュータがコンピュータ資源あるいはネットワーク資源を使用する場合において用いられ、システムにより生成される構成情報を参照するステップと、構成情報を基に、あらかじめ準備される複数の認証方式のうちのいずれか選択するステップと、入力されるユーザ識別子とパスワードにより、選択された認証方式に従うセキュリティチェックを行うステップとがプログラムされ記録されることも特徴とする。

【００１０】このことにより、セキュリテイの一括管理を実現でき、必要のない資源をアクセスすることなくセキュリティ機能の充実がはかれるとともに、ユーザからは常に同じ入力内容にて様々なアクセス権を行使できる。

【００１１】

【発明の実施の形態】図1は本発明の認証システムの構成例を示すブロック図である。図において、符号1は認証サーバ、符号２、３はクライアントコンピュータであり、両者はネットワーク回線4を介して接続されている。５は大容量記憶外部記憶装置であり、クライアントコンピュータ２により参照される。本発明は、特徴的には、クライアントコンピュータ２（３）中に、セキュリティチェックディスパッチャＳＣＤ２１とプロパティジェネレータＰＧ２５を持つ。

【００１２】ＳＣＤ２１は、そのコンピュータ２（３）が、コンピュータ資源あるいはネットワーク資源を使用する場合、ユーザ識別子とパスワードの他にその属性情報を含むネットワーク情報の入力を促し、入力される属性情報あるいはＰＤ２５に従う構成情報に従い、あらかじめ準備される複数の認証方式のうちいずれかを選択し、あらかじめ用意されるコンピュータ認証プロセッサ２３あるいはネットワーク認証プロセッサ２２を起動し、選択された認証方式に従うセキュリティチェックを行うものである。各構成の詳細については後述する。

【００１３】図2にクライアントコンピュータ２，３にインプリメントされるソフトウェア構造を示す。図2は、本発明実施形態にて使用されるソフトウェアの構造をクライアントコンピュータが持つメモリ上にマッピングして示した図である。図において、符号２１は、セキュリティチェックディスパッチャ（ＳＣＤ）であり、ここで、ユーザに対してユーザ識別子２１０１とパスワード２１０２ならびにその属性情報２１０３を含むネットワーク情報２１０の入力を促す。符号２２，２３は、それぞれ、ネットワーク資源の認証、コンピュータ内資源

5

の認証を行なうためにあらかじめ用意されるプロセッサ（それぞれ、ネットワーク認証プロセッサ２２、コンピュータ認証プロセッサ２３）であり、ＳＣＤ２１が上述したユーザ入力に従う属性情報２１０３によりいずれか一方を選択して起動する。例えば、ネットワーク認証プロセッサ２２は、そのネットワーク情報２１０をネットワーク回線4 経由で認証サーバ1 へ送って認証を確認し、コンピュータ認証プロセッサ２３では、自身で持つパスワードデータベース２４を参照することにより認証を確認する。

【００１４】ネットワーク情報２１０のうち、属性情報のみユーザ入力に依存せず、コンピュータ２（３）により自動生成することも可能である。即ち、プロパティジェネレータ（ＰＧ２５）による構成情報の自動生成を利用するものである。ＰＧ２５は、コンピュータが通常持つ構成調査プログラムが持つ機能を拡張したものであり、ＰＧ２５は、ネットワーク４をアクセスしてそのコンピュータ２が正しくネットワーク接続されていることを確認し、接続がなされていた場合、属性情報２１０３としてネットワークアクセスを選択する情報に設定する。そして、ＳＣＤ２２にコントロールを移し、ネットワークによる認証が許可された場合は、コンピュータ２内の資源を含むアクセス権を与えるようにする。また、接続がなされていなかった場合にはネットワークアクセスを禁止する情報を設定し、コンピュータ内資源のみのアクセス権を与えるようにする。資源のアクセス権を簡単に、かつ、統一したセキュリティ方式で管理できる。

【００１５】図3 は上述した本発明の実施形態の具体的動作を記述したフローチャートであり、具体的にはＳＣＤ２１によるプログラム処理の流れが示されている。ＳＣＤ２１は、セキュリティチェックの際、図4 に示す表示画面生成（ステップＳ１）を行い、ユーザに対し、ＩＤ、パスワードの他、属性情報の入力を促す（ステップＳ２）。ここでは、属性情報として、画面に表示されたチェックボックスのＮｅｔ，Ｌｏｃａｌ を選択指示するものとする。Ｎｅｔ が選択された場合、コンピュータ資源を含むネットワークアクセスを、Ｌｏｃａｌ が選択された場合、コンピュータ資源のアクセスのみを意志表示しているものとする。

【００１６】ＳＣＤ２１は、更に構成情報の存在をチェック（ステップＳ３）し、あれば（ステップＳ３の有）、ＰＧ２５による構成情報を参照（ステップＳ４）し、ネットワーク認証プロセッサ２２，コンピュータ認証プロセッサ２３の一方、あるいは両方を選択し、適切なセキュリティチェック（ステップＳ６）を行なう。構成情報がなければ（ステップＳ３の無）、ユーザからの属性情報入力に従う、Ｎｅｔ あるいはＬｏｃａｌ をチェック（ステップＳ５）し、適切なセキュリティチェックを行なう。

【００１７】以上のように制御することで、ユーザに対し特に負担を強いることなく最適な認証方式を選択でき、また、ネットワーク資源を利用する必要がない場合、属性情報を変えるだけで最適な認証が可能となり、不必要なネットワークアクセスを行なうことがなくなる。

【００１８】

【発明の効果】以上説明のように本発明は、コンピュータがコンピュータ資源あるいはネットワーク資源を使用する場合、ユーザ識別子とパスワードの他にその属性情報を含むネットワーク情報の入力を促し、入力される属性情報あるいは構成情報に従い、あらかじめ準備される複数の認証方式のうちいずれかを選択し、選択された認証方式に従うセキュリティチェックを行うものであり、このことにより、ネットワーク資源を利用する必要がない場合には、属性情報あるいは構成情報を変更するだけで認証が可能となり、不要なネットワークアクセスを生じることはない。従って、パスワード盗難の機会が減り、ユーザからは常に同じ入力内容にて様々なアクセス権を行使できるものである。

【図面の簡単な説明】

【図1】本発明の認証システムの構成例を示すブロック図、

【図2】図1 に示すクライアントコンピュータにインプリメントされるソフトウェアの構造をメモリ上に展開して示した図、

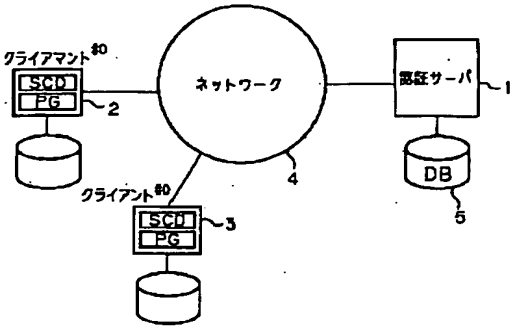
【図3】本発明実施形態の動作を説明するために引用したフローチャート、

【図4】本発明にて使用されるパスワード入力画面の例を示す図、

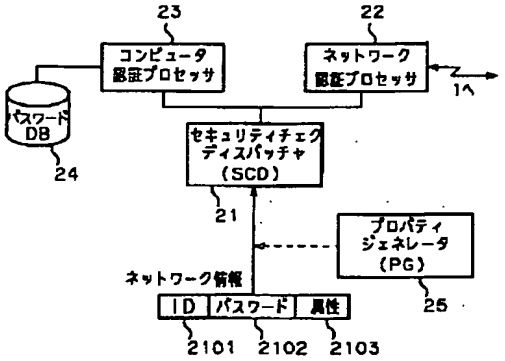
【符号の説明】

１…認証サーバ、２（３）…クライアントコンピュータ、４…ネットワーク回線、５…認証データベース、２１…セキュリティチェックディスパッチャ（ＳＣＤ）、２２…ネットワーク認証プロセッサ、２３…コンピュータ認証プロセッサ、２４…パスワードデータベース、２５…プロパティジェネレータ（ＰＧ）。

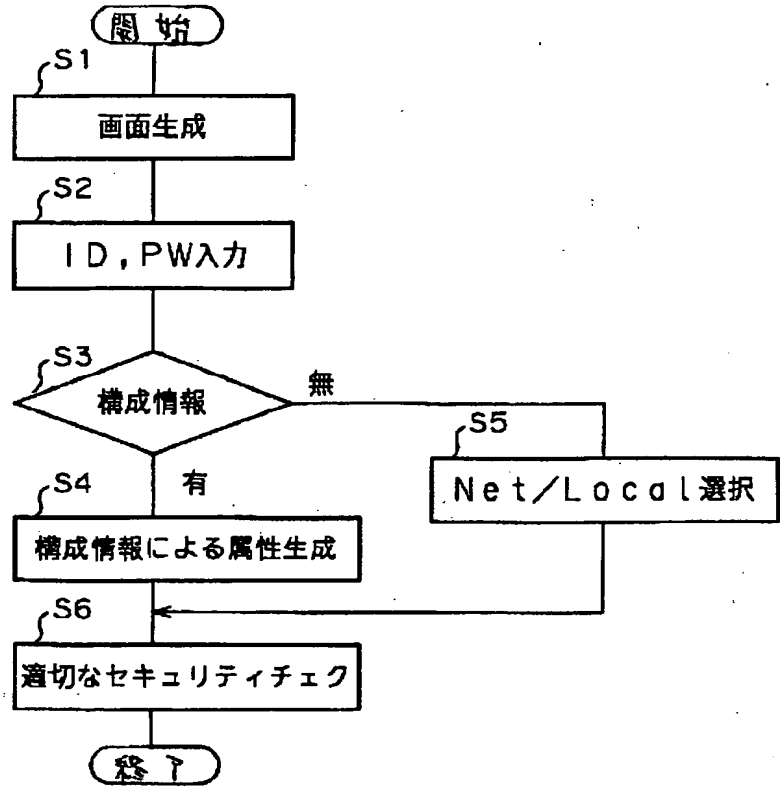
【 図1 】


クライアント#0
SCD
PG
2
ネットワーク
認証サーバ
1
4
DB
5
クライアント#0
SCD
PG
3

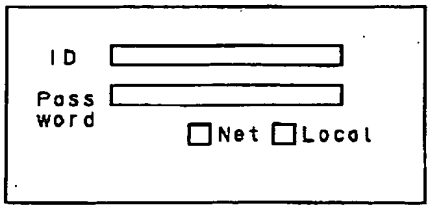
【 図2 】


23
22
コンピュータ認証プロセッサ
ネットワーク認証プロセッサ
1へ
パスワードDB
24
セキュリティチェックディスパッチャ(SCD)
21
プロパティジェネレータ(PG)
ネットワーク情報
ID
パスワード
属性
25
2101
2102
2103

【 図3 】


開始
S1
画面生成
S2
ＩＤ，ＰＷ入力
S3
構成情報
無
S5
Ｎｅｔ／Ｌｏｃａｌ選択
S4
有
構成情報による属性生成
S6
適切なセキュリティチェク
終了

【 図4 】


ID
Pass word
Net
Local